

UNITED STATES PATENT AND TRADEMARK OFFICE  
**CERTIFICATE OF CORRECTION**

PATENT NO. : 7,231,040 B1  
APPLICATION NO. : 09/328726  
DATED : June 12, 2007  
INVENTOR(S) : Thomas Collins et al.

Page 1 of 4

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

In column 2, line 27, after "is" insert -- a --.

In column 2, line 32 (equation 6), delete " $e \cdot d \equiv 1 \pmod{1 \text{ cm}(p-1), (q-1))}$ " and insert --  $e \cdot d \equiv 1 \pmod{1 \text{ cm}((p-1), (q-1))}$  --, therefor.

In column 7, line 6, above "k is the number" insert -- where  $w_i = \prod_{j=1}^i p_j$ , and --.

In column 10, line 39, above "Each block M" delete " $0 \leq M \leq N-1$ ."

In column 12, line 20, in Claim 10, after " $p_2, \dots$ " delete "and".

In column 13, line 49, in Claim 19, delete "steps" and insert -- step --, therefor.

In column 15, line 19, in Claim 28, after "of" delete ":".

In column 15, line 46, in Claim 29, after "claim 28" delete " , ".

In column 16, line 62, in Claim 37, delete " $M_1' \equiv C_1^{d1} \pmod{p_1}$ ," and insert --  $M_1' \equiv C_1^{e1} \pmod{p_1}$ , --, therefor.

In column 16, line 64, in Claim 37, delete " $M_2' \equiv C_2^{d2} \pmod{p_2}$ ," and insert --  $M_2' \equiv C_2^{e2} \pmod{p_2}$ , --, therefor.

In column 16, line 67, in Claim 37, delete " $M_k' \equiv C_k^{dk} \pmod{p_k}$ ," and insert --  $M_k' \equiv C_k^{ek} \pmod{p_k}$ , --, therefor.

In column 19, line 48, in Claim 56, after "wherein" insert -- , --.

In column 19, line 53, in Claim 56, after " $p_2, \dots$ " insert -- , --.

In column 19, line 67, in Claim 56, after "with" insert -- , --.

In column 20, line 62, in Claim 64, delete "steps" and insert -- step --, therefor.

UNITED STATES PATENT AND TRADEMARK OFFICE  
**CERTIFICATE OF CORRECTION**

PATENT NO. : 7,231,040 B1  
APPLICATION NO. : 09/328726  
DATED : June 12, 2007  
INVENTOR(S) : Thomas Collins et al.

Page 2 of 4

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

In column 22, line 14, in Claim 70, delete "numbers" and insert -- number --, therefor.

In column 22, line 15, in Claim 70, delete "number" and insert -- numbers --, therefor.

In column 22, line 33, in Claim 73, after " $p_k$ " insert -- , --.

In column 22, line 39, in Claim 73, delete "signal" and insert -- signed --, therefor.

In column 22, line 42, in Claim 73, after "with" insert -- , --.

In column 22, line 60 in Claim 73, delete " $d \equiv e^{-1} \bmod (p_1-1) (p_2-1) \dots (p_k-1)$ " and insert --  $d \equiv e^{-1} \bmod ((p_1-1) (p_2-1) \dots (p_k-1))$  --, therefor.

In column 23, line 61, in Claim 82, after " $p_2, \dots$ " insert -- , --.

In column 23, line 66, in Claim 82, delete "C, whereby" and insert -- C whereby, --, therefor.

In column 24, line 2, in Claim 82, delete " $d \equiv e^{-1} \bmod (p_1-1) (p_2-1) \dots (p_k-1)$ " and insert --  $d \equiv e^{-1} \bmod ((p_1-1) (p_2-1) \dots (p_k-1))$  --, therefor.

In column 24, line 9, in Claim 82, delete " $M_1' \equiv C_1^{d1} \bmod p_1$ ," and insert --  $M_1' \equiv C_1^{e1} \bmod p_1$ , --, therefor.

In column 24, line 11, in Claim 82, delete " $M_2' \equiv C_2^{d2} \bmod p_2$ ," and insert --  $M_2' \equiv C_2^{e2} \bmod p_2$ , --, therefor.

In column 24, line 14, in Claim 82, delete " $M_k' \equiv C_k^{dk} \bmod p_k$ ," and insert --  $M_k' \equiv C_k^{ek} \bmod p_k$ , --, therefor.

In column 25, line 22, in Claim 91, after " $p_2, \dots$ " insert -- , --.

In column 26, line 9, in Claim 92, after " $p_2, \dots$ " insert -- , --.

In column 26, line 59, in Claim 93, delete "steps" and insert -- step --, therefor.

UNITED STATES PATENT AND TRADEMARK OFFICE  
**CERTIFICATE OF CORRECTION**

PATENT NO. : 7,231,040 B1  
APPLICATION NO. : 09/328726  
DATED : June 12, 2007  
INVENTOR(S) : Thomas Collins et al.

Page 3 of 4

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

In column 26, line 67, in Claim 93, after " $p_2, \dots$ " insert -- , --.

In column 27, line 33, in Claim 94, after "C" insert -- , --.

In column 27, line 40, in Claim 94, after " $p_2, \dots$ " delete "and".

In column 28, line 15, in Claim 95, after " $p_2, \dots$ " insert -- , --.

In column 29, line 8, in Claim 96, after "said" delete "decoding".

In column 29, line 14, in Claim 96, after "with" insert -- , --.

In column 29, line 37, in Claim 97, delete "steps" and insert -- step --, therefor.

In column 29, line 45, in Claim 97, after " $p_2, \dots$ " insert -- , --.

In column 30, line 21, in Claim 98, after " $p_k$ " insert --  $k$  --.

In column 30, line 22, in Claim 98, after " $p_2, \dots$ " insert -- , --.

In column 30, line 22, in Claim 98, after " $p_k, \dots$ " insert -- , --.

In column 30, line 31, in Claim 98, delete "of;" and insert -- of, --, therefor.

In column 30, line 32, in Claim 98, after "with" insert -- , --.

In column 30, line 67, in Claim 99, after " $p_2, \dots$ " insert -- , --.

In column 31, line 4, in Claim 99, delete "C, whereby" and insert -- C whereby, --, therefor.

In column 32, line 7, in Claim 100, after " $p_2, \dots$ " insert -- , --.

UNITED STATES PATENT AND TRADEMARK OFFICE  
**CERTIFICATE OF CORRECTION**

PATENT NO. : 7,231,040 B1  
APPLICATION NO. : 09/328726  
DATED : June 12, 2007  
INVENTOR(S) : Thomas Collins et al.

Page 4 of 4

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

In column 32, line 20, in Claim 100, delete "signal" and insert -- signed --, therefor.

Signed and Sealed this

Second Day of September, 2008

A handwritten signature in black ink, reading "Jon W. Dudas". The signature is stylized, with a large, looped initial "J" and a distinct "D" at the end.

JON W. DUDAS  
*Director of the United States Patent and Trademark Office*